

AMENDMENTS TO THE CLAIMS

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

Listings of the Claims

1 – 2. (Canceled)

3. (Withdrawn) A method for establishing a common key for a group of at least three subscribers, the method comprising:

generating by each subscriber T_i of the at least three subscribers a respective message $N_i = (g^{z_i} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G and a respective random number z_i and sending the respective message from the respective subscriber to all other subscribers T_j of the at least three subscribers, each respective random number z_i being selected or generated by the respective subscriber T_i ;

generating by each subscriber T_i a transmission key k^i from the messages N_j received from the other subscribers T_j , $j \neq i$, and the respective random number z_i according to $k^i = N_j^{z_i} = (g^{z_j})^{z_i}$; sending by each subscriber T_i the respective random number z_i in encrypted form to all other subscribers T_j by generating the message M_{ij} according to $M_{ij} := E(k^i, z_i)$, $E(k^i, z_i)$ being a symmetrical encryption algorithm in which the data record z_i is encrypted with the transmission key k^i ; and

determining a common key k by each subscriber T_i using the respective random number z_i and the random numbers z_j , $j \neq i$, received from the other subscribers according to

$k := f(z_1, \dots, z_n)$,

f being a symmetrical function which is invariant under a permutation of its arguments.

4. (Withdrawn) The method as recited in claim 3 wherein the transmission key k^i is known to subscriber T_j according to $k^i = k^j$.

5. (Currently Amended) A method for establishing a common key for a group of at least three subscribers for transmitting messages over a communication channel, the method comprising the steps of:

generating, by each subscriber T_j , a respective message $N_j = (g^{z_j} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G and a respective random number z_j , $j = 1$ to n , where n is the number of subscribers in the group of at least three subscribers;

sending the respective message N_j by each subscriber except a predetermined first subscriber T_1 of the at least three subscribers, to each of the other subscribers T_j , $j \neq 1$ the first subscriber T_1 .

encrypting, by the a first subscriber T_1 , the received messages N_j of the other subscribers T_j , $j \neq 1$, with the random number z_1 to form a respective transmission key k^{1j} for each subscriber $T_j, j \neq 1$.

computing, by each subscriber T_j , $j \neq 1$, a symmetrical counterpart k^{1j} of the respective transmission key k^{11} using the received message N_1 :

sending, by the first subscriber T_1 , the random number z_1 to all other subscribers $T_j, j \neq 1$ in encrypted form by generating a message M_{1j} according to $M_{1j} := E(k^{1j}, z_1)$, $E(k^{1j}, z_1)$ being a symmetrical encryption algorithm in which the random number z_1 is encrypted with the transmission key k^{1j} , and

decrypting, by each subscriber T_i , the message M_{ij} :

determining a common key k , by each subscriber T_j , using an assignment $k := h(z_1, g^{x_2}, \dots, g^{x_n})$, $h(x_1, x_2, \dots, x_n)$ being a function which is symmetrical in the arguments x_2, \dots, x_n [1].

encrypting, by one of the subscribers T_i , a transmission message using the common key k_i ; and being useable for transmitting messages over a communication channel

transmitting the encrypted transmission message to at least one of the other subscribers T_{j-i} ≠ i .

6. (Previously Presented) The method as recited in claim 5 wherein the transmission key is known to subscriber T_j according to $k^{ij} = k^{ji}$.

7. (Currently Amended) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number z_j , where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j generating a respective first message $N_j = (g^{z_j} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G ;

each of the subscribers $T_j, j \neq 1$, sending the respective first message N_j to a first subscriber T_1 , each of the other subscribers $T_i, j \neq i$;

the a first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z_1} \bmod p$ for each of the other subscribers $T_j, j \neq 1$, based on the received respective first message $N_j, j \neq 1$;

each of the subscribers $T_i, i \neq 1$, computing a symmetrical counterpart k^{ji} of the respective transmission key k^{1i} using the received first message N_1 ;

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z_1)$ for each of the other subscribers T_j , $j \neq 1$, where $E(k^{1j}, z_1)$ is a symmetrical encryption algorithm in which z_1 is encrypted with the transmission key k^{1j} ;

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the other subscribers T_j , $j \neq 1$; and

each of the subscribers T_j decrypting the second message M_{1j} ;

each of the subscribers T_j computing a common key k according to an assignment $k := h(z_1, g^{x_1}, \dots, g^{x_n})$, where $h(x_1, x_2, \dots, x_n)$ is a symmetrical function;

a subscriber T_i encrypting a third message using the common key k ; and

the subscriber T_i transmitting the encrypted third message to at least one of the other subscribers T_j , $j \neq i$;

8. (Currently Amended) The method according to claim 7, wherein the each respective random number z_j is selected from the set $\{1, \dots, p-2\}$.

9. (Previously Presented) The method according to claim 7, wherein the length of p is at least 1024 bits.

10. (Previously Presented) The method according to claim 7, wherein g has a multiplicative order of at least 2^{160} .

11. (Previously Presented) The method according to claim 7 wherein the transmission key is known to a respective subscriber T_j according to $k^{ij} = k^{jl}$.

12. (Previously Presented) The method according to claim 7, wherein $h(z_1, g^{z_2}, \dots, g^{z_n}) = g^{z_1 * z_1} * g^{z_2 * z_1} * \dots * g^{z_n * z_1}$.

13. (Currently Amended) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number z_j , where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j storing the respective random number z_j in a respective memory;

each of the subscribers T_j generating a respective first message $N_j = (g^{z_j} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G ;

each of the subscribers $T_j, j \neq 1$, sending the respective first message $N_j, j \neq 1$ to a first subscriber T_1 each of the other subscribers $T_j, j \neq j$;

the first subscriber T_1 storing each of the received first messages $N_j, j \neq 1$ in a memory;

the first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z_1} \bmod p$ for each of the other subscribers $T_j, j \neq 1$, based on the received respective first message $N_j, j \neq 1$;

each of the subscribers $T_j, j \neq 1$, computing a symmetrical counterpart k^{j1} of the respective transmission key k^{1j} using the received first message N_{1j}

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z1)$ for each of the other subscribers T_j , $j \neq 1$, where $E(k^{1j}, z1)$ is a symmetrical encryption algorithm in which $z1$ is encrypted with the transmission key k^{1j} ;

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the respective other subscribers T_j , $j \neq 1$;

each of the respective other subscribers subscribers T_j , $j \neq 1$, storing the received encrypted second message in the respective memory; and

each of the subscribers T_j decrypting the second message M_{1j} ;

each of the subscribers T_j computing a common key k according to an assignment $k := h(z1, g^{j1}, \dots, g^{jn})$, where $h(x1, x2, \dots, xn)$ is a symmetrical function, and n is the number of subscribers subscribers in the group;

one of the subscribers T_i encrypting a third message using the common key k ; and

the subscriber T_i transmitting the encrypted third message to at least one of the other subscribers T_j , $j \neq i$.

14. (Currently Amended) The method according to claim 13, wherein whereby a maximum number of transmission rounds required is two.

15. (Currently Amended) The method according to claim 13, further comprising the steps of:

one of the respective subscribers T_i using the computed common key k to encrypt a third message;

the one of the respective subscribers subscriber T_i transmitting the encrypted third message to each of the other respective subscribers $T_j, j \neq i$;

each of the other respective subscribers $T_j, j \neq i$ decrypting the received encrypted third message using the computed common k .

16. (New) The method according to claim 5, further comprising the step of:

decrypting, by the at least one of the other subscribers $T_j, j \neq i$, the transmitted transmission message using the common key k .

17. (New) The method according to claim 7, further comprising the step of:

the at least one other subscriber $T_j, j \neq i$ decrypting the received third message using the common key k .

18. (New) The method according to claim 13, further comprising the step of:

the at least one other subscriber $T_j, j \neq i$ decrypting the received third message using the common key k .